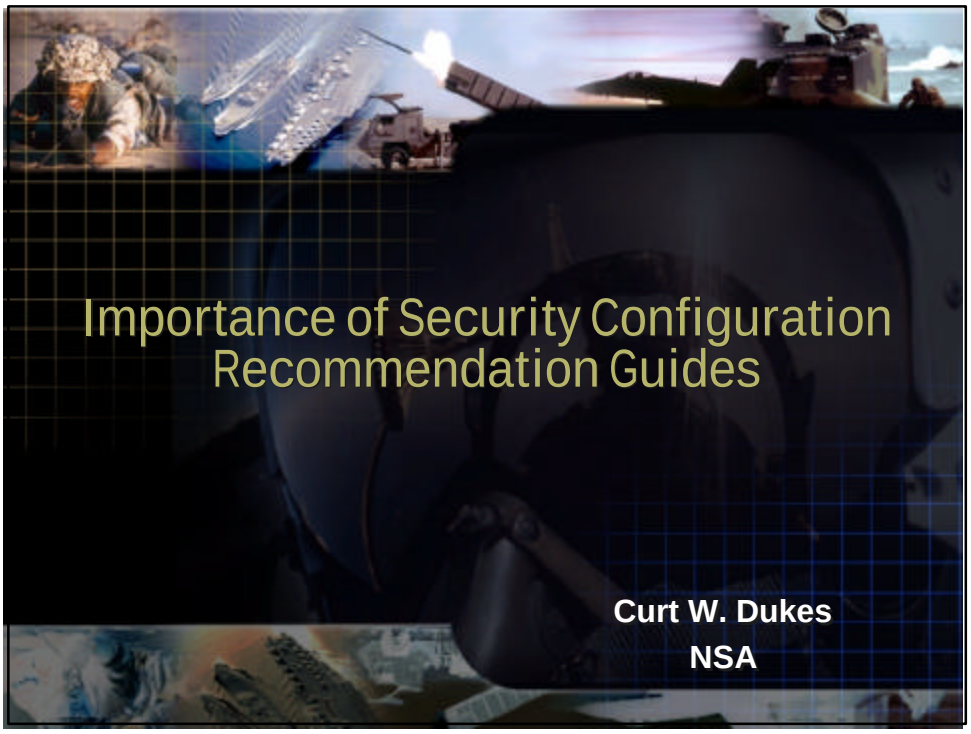
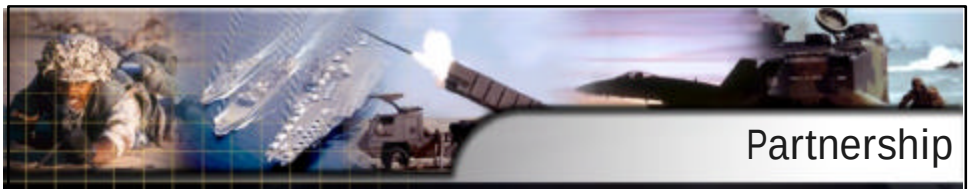
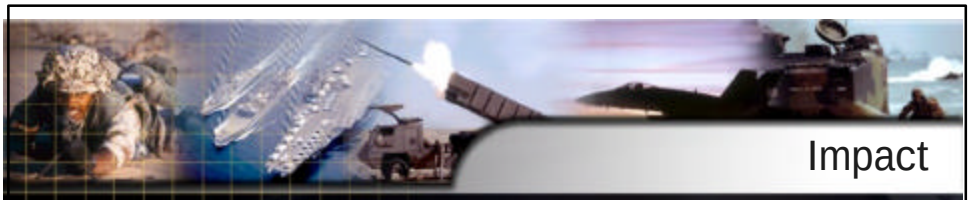

Importance of Security Configuration Recommendation Guides
Curt W. Dukes
NSA


NSA Security Configuration Guides
MS Windows NT Guide – 1997
MS Windows 2000 Security Recommendation Guides – 2001
27 people – 11 months – NSA + DISA
Microsoft, CIS, others beta test
Cisco Secure Router Configuration Guide – 2001
12 people – 10 months
Cisco, CIS beta test
MS Windows 2003 Server – 2003
NSA endorsement



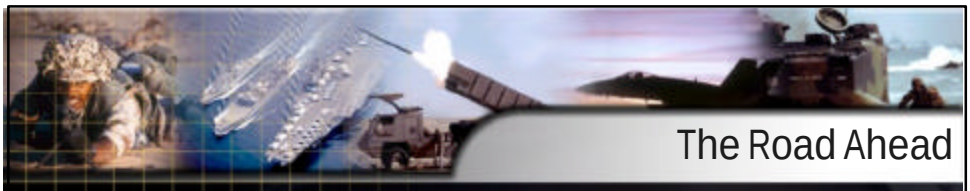
Partnership

- Shared problem, shared solutions
- DISA
  - *Security Technical Implementation Guidance*
- Center for Internet Security
  - *Benchmarks*
  - *Tools to check configuration and guide administrator*
- SANS Institute
- Industry
  - *Bindview*
  - *Microsoft*
  - *Cisco*



Impact

- DoDCERT – 93% of compromises in 2002 exploited known vulnerabilities
- NSA Tests – MS Windows 2000 Benchmark + MS Patches close 80-90% of know vulnerabilities
- Private Sector case studies show similar improvements
- U.S. Infrastructure – Wide Improvement
  - *Big bang for little buck*

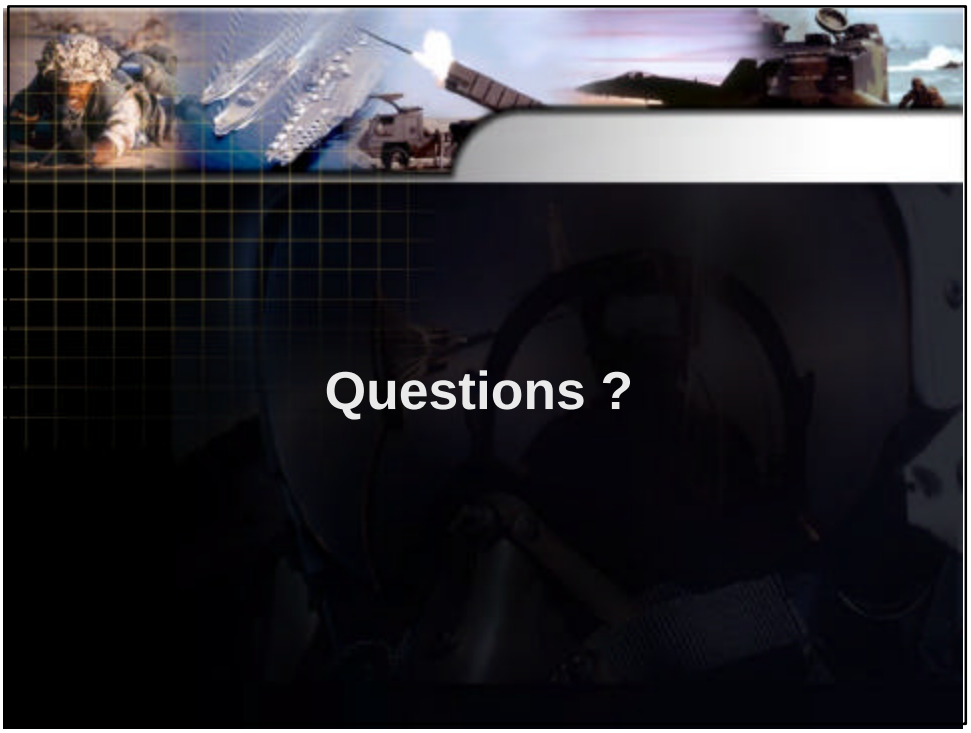


The Road Ahead

- **Policy Possibilities of Benchmarks**
  - *Define Robustness Requirements of DoDI 8500*
  - *Support DITSCAP process. Tailor Benchmarks to classes*
  - *Specify Security Requirements in Acquisition*
- **Prove the Concept**
  - *Test DoD Applications – DMS*
  - *Benchmark Operational Systems – Then Red Team*
  - *Develop Tools that apply benchmarks and check compliance*
- **Leverage Community Partnership**

Summary

- **Expertise and agreement of leading IT security specialists**
- **A "vendor-friendly" definition of security**
- **An achievable level of "minimum security hygiene"**
- **A target for a rich tool set to help manage security**
  - *CIS tools are the first step*
  - *Vendors also rising to the challenge*


Questions ?